CLAIMS

What is claimed is:

1. A method for performing a cryptographic operation on a message, comprising:
   (a) generating initial unpredictable information;
   (b) using said initial unpredictable information, transforming an initial secret quantity into a plurality of randomized quantities having a predetermined logical relationship thereamong; and
   (c) performing a first step of said operation involving said randomized quantities in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device.

2. The method of Claim 1 wherein said initial unpredictable information includes a plurality of random values obtained from a random number generator.

3. The method of Claim 1 wherein said initial secret quantity includes at least one of the group of secret quantities comprising a message and a key.

4. The method of Claim 1 wherein step (b) includes a blinding operation.

5. The method of Claim 4 wherein said blinding operation includes an XOR operation.

6. The method of Claim 1 wherein the probability that the value of any specific bit in any of said randomized quantities is a "one" is one half (0.5).

7. The method of Claim 1 wherein step (c) includes separately operating on a plurality of said randomized quantities in a random order.

8. The method of Claim 1 wherein said cryptographic operation is compatible with the Data Encryption Standard (DES), said method further comprising recombining the result of step (c) to produce a final result, said final result being a cryptographic representation of said message transformed with said DES algorithm.

9. The method of Claim 8 further comprising using said initial unpredictable information to shuffle the S tables.

10. The method of Claim 9 wherein said step of using said initial unpredictable information to shuffle said S tables includes blinding the outputs of said S tables.

11. The method of Claim 9 wherein said step of using said initial unpredictable information to shuffle said S tables includes permuting said S tables.

12. The method of Claim 9 wherein step (c) includes extracting, in random order, data representing the six-bit inputs to the S tables in randomized form from said randomized quantities.

13. The method of Claim 1 further comprising:

(d) updating at least one of said randomized quantities using additional unpredictable information to generate at least one updated randomized quantity; and

(e) performing a second step of said operation involving said at least one updated randomized quantity.

14. The method of Claim 13 wherein step (d) includes reordering the bit positions of said at least one randomized quantity.

15. The method of Claim 13 wherein step (d) includes randomizing the bit values of said at least one randomized quantity.

16. The method of Claim 13 wherein step (d) includes incrementing and checking a failure counter prior to said updating, and clearing said failure counter following said updating.

17. The method of Claim 13 wherein step (c) includes performing said first step of said operation using a plurality of parameters, said method further comprises using said initial unpredictable information to initialize said parameters and updating said parameters to generate a plurality of updated parameters, and step (e) includes performing said second step of said operation using said updated parameters.

18. A method for performing a cryptographic operation on a message using a key, comprising:

(a) using unpredictable information, transforming said message into a plurality of message portions having a predetermined logical relationship thereamong;

(b) using unpredictable information, transforming said key into a plurality of key portions having a predetermined logical relationship thereamong;

(c) performing a first step of said cryptographic operation on said message portions using said key portions in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device;

(d) updating at least one of said plurality of message portions with unpredictable information;

(e) updating at least one of said plurality of key portions with unpredictable information;

(f) performing at least a second step of said cryptographic operation on said message portions using said key portions in a hardware device to reduce the amount of useful information about said operation available from external monitoring of said hardware device; and

(g) returning a cryptographic result.

19. The method of Claim 18 wherein said cryptographic operation is compatible with the Data Encryption Standard (DES) such that said result is a representation of the value derived by applying the DES algorithm to said message.

20. The method of Claim 18 further comprising a step of using unpredictable information to reshuffle the S tables between step (c) and step (f).

21. The method of Claim 18 wherein said step (b) establishes a predefined mathematical relationship between said key portions and said secret quantity which is preserved when said key portions are updated at step (e).

22. A cryptographic processing device for performing a cryptographic operation in a manner resistant to discovery of a secret quantity by external monitoring, comprising:

(a) an untrusted input for electrical power, from which the device's power consumption can be measured;

(b) a secure memory containing at least a representation of said secret quantity;

(c) a source of unpredictable information for transforming said secret quantity into a plurality of randomized quantities having a predetermined logical relationship thereamong;

(d) an input/output interface;

(e) a processor connected to said memory, configured to perform cryptographic transformations on randomized forms of data received via said interface using randomized forms of said secret quantity.

23. The device of Claim 22 wherein said device comprises an ISO 7816 compliant smartcard.

24. The device of claim 22 wherein said power consumption varies measurably during said cryptographic transformations, but where measurements of said power consumption are not correlated to said secret quantity.

25. The device of Claim 22 wherein said source of unpredictable information comprises a random number generator.

26. The device of Claim 22 further comprising at least one register for temporarily storing said randomized quantities, wherein the correlation between any single bit of said at least one register and said secret quantity is undetectably small, but where the correlation between a combination of multiple bits of said at least one register and said secret quantity is measurably significant.

27. The device of Claim 26 wherein said device is an ISO 7816 compliant smartcard.

28. A method for performing a symmetric cryptographic operation using a secret key with resistance to external monitoring attacks, comprising:

(a) obtaining an input message;

(b) generating initial unpredictable information;

(c) combining said key, said message, and said unpredictable information;

(d) deriving a result, where:

(i) said result is a predefined function of said input message and of said key, and

(ii) said result is independent of said unpredictable information; and

(e) producing a response based on said result.

29. The method of Claim 28 wherein said cryptographic operation is a predefined block cipher.

30. The method of claim 29 wherein said block cipher is the Data Encryption Standard.

31. The method of claim 29 wherein all steps are implemented in an ISO 7816-compliant smartcard.

32. The method of claim 29 wherein individual no bit manipulated in said step (d) is measurably correlated to any bit of said key.

33. A device for performing keyed cryptographic operations, comprising:

(a) a keyed processing unit, configured to

(i) obtain a representation of a secret parameter encoded as a first plurality of parameters,

(ii) receive an input datum,

(iii) perform a cryptographic operation upon said input datum using said plurality of parameters, and

(iv) transmit the result of said cryptographic operation; and

(b) a key update unit, configured to

(i) obtain said encoded representation of said secret parameter,

(ii) obtain a blinding factor,

(iii) produce from said first plurality of parameters and said blinding factor a second plurality of parameters where

(1) a mathematical relationship exists between said second plurality of parameters and said first plurality of parameters; and

(2) said second plurality of parameters is different from said first plurality of parameters

34. The device of claim 33 where said key preparation unit is further configured to derive a plurality of parameters from said secret parameter and said blinding value such that a mathematical relationship exists between said derived plurality of parameters and said obtained secret parameter, but where no measurable correlation is present between any one of said plurality of parameters and said secret parameter.

35. The device of claim 34 where said mathematical relationship includes addition modulo 2.

36. The device of claim 33 where said second plurality of parameters includes

(a) A permuted part, containing a sequence of bits in permuted order; and

(b) An ordering part, which contains the order of bits in said permuted part

37. A method for reducing the correlation between physical attributes of a cryptographic system and the values of secret parameters being manipulated during a cryptographic operations, by masking a table lookup operation, consisting of the following steps:

(a) receiving a representation of a lookup table for use in said table lookup operation;

(b) receiving input and output masking parameters corresponding to said received table representation;

(c) obtaining some unpredictable information;

(d) deriving a transformed representation of said lookup table from said received lookup table and said unpredictable information;

(e) deriving new input and output masking parameters corresponding to said transformed representation of said table;

(f) storing said transformed lookup table and said input and output masking parameters in a memory; and

(g) using said transformed table in a cryptographic computation.

38. The method of claim 37 where step (d) includes the following substeps:

(a) obtaining a first random value;

(b) generating a new output masking value from said first random value and an output masking value received at step (b);

(c) obtaining a second random value;

(d) generating a new input masking value from said second random value and an input masking value received at step (b);

(e) producing said transformed table with the property that the i^{th} element in the transformed table is equal to the result of

(i) finding the element at the location in the original table specified by taking an index 'i' XORed with said old input mask,

(ii) XORing said element with the values of both said new output mask and said old output mask

(iii) storing said XOR result in said transformed table at a location corresponding to said index 'i' XORed with said new input mask

39. The method of claim 38 where the steps are performed in a different order.

40. A method for transforming data in a smartcard using the Data Encryption Standard with a secret key, comprising the steps of:

(a) receiving a representation of a message;

(b) combining at least a portion of said message representation with at least a portion of a representation of said key to produce a DES intermediate representation;

(c) producing from said DES intermediate an index to an S operation, where said index is a representation of a traditional 6-bit S table input;

(d) performing an S operation, producing an S result in an expanded representation for which the Hamming Weight of said S result is independent of the value of said S table input;

(e) combining the result of said S operation with said DES intermediate to produce a new DES intermediate representation;

(f) repeating steps (c) through (e) a plurality of times; and

(g) converting the final DES intermediate representation into a DES result, where said DES result is a representation of the result of applying the DES standard to said message with said secret key.

Add A3